

Application No. 09/943,889  
Response to Office Action

Customer No. 01933

REMARKS

Reconsideration of this application, as amended, is respectfully requested.

THE CLAIMS

Independent claims 1, 6 and 8 have been amended to clarify the features of the present invention whereby the variable parameter used in generating the second key is received from the user terminal, and whereby the H/W key ID used in generating the second key is retrieved from a user information database by using a user ID received from the user terminal. See Figs. 3 and 4 and the disclosure in the specification at page 7, lines 18-23 and at page 8, lines 25-27.

In addition, claim 2 has been amended to better accord with amended claim 1, and claim 3 has been canceled.

Still further, claims 1, 2, 4 and 6-9 have been amended to make some minor grammatical improvements so as to put them in better form for issuance in a U.S. patent.

And yet still further, new claims 10-12 have been added to recite the feature of the present invention whereby the contents information of the contents data comprises a size of the contents data and a preceding update date of the contents data, as

Application No. 09/943,889  
Response to Office Action

Customer No. 01933

supported by the disclosure in the specification at page 8,  
lines 19-21.

No new matter has been added, and it is respectfully  
requested that the amendments to claims 1, 2, 4 and 6-9 and the  
addition of new claims 10-12 be approved and entered.

THE PRIOR ART REJECTION

Claims 1-9 were rejected under 35 USC 103 as being obvious  
in view of USP 6,636,968 ("Rosner et al"). This rejection,  
however, is respectfully traversed with respect to the claims as  
amended hereinabove.

On page 2 of the Office Action, the Examiner asserts that  
Rosner et al discloses generating a first key at the server from  
contents information of the contents data to be distributed at  
column 3, lines 51-60 thereof.

It is respectfully submitted, however, that the cited  
portion of Rosner et al describes the creation of partial  
keys 225, 226 and 227, which are used in decrypting encrypted  
content material, such that knowledge of the private key of the  
destination device and knowledge of a common group key  
facilitates determination of a decryption key. That is, it is  
respectfully submitted that the cited portion of Rosner et al  
relates to the formation of the decryption key (which the

Application No. 09/943,889  
Response to Office Action

Customer No. 01933

Examiner apparently considers to correspond to the first key of the present invention) at the destination devices, and not at the server.

In addition, it is respectfully pointed out that Rosner et al discloses that the session key K 221, which corresponds to the decryption key formed at the destination devices, is formed at the source device 210 based on the secret key x of the source device 210 and the public keys 251a, 261a, 271a, etc. of the destination devices. See column 3, lines 42-50 of Rosner et al.

Still further, it is respectfully submitted that Rosner et al does not at all disclose, teach or suggest contents information of the contents data to be distributed, as recited in independent claims 1, 6 and 8.

Thus, it is respectfully submitted that Rosner et al clearly does not disclose, teach or suggest generating the first key based on contents information of the contents data to be distributed, whether at the destination device (as in the portion of Rosner et al cited by the Examiner) or at the server (as recited in independent claims 1, 6 and 8).

As recited in new claims 10-12, moreover, the contents information comprises a size of the contents data and a preceding update date of the contents data. And it is respectfully submitted that Rosner et al clearly does not disclose, teach or

Application No. 09/943,889  
Response to Office Action

Customer No. 01933

even remotely suggest these features of the present invention as recited in new claims 10-12.

In addition, it is respectfully submitted that Rosner et al does not disclose, teach or suggest generating a second key at the server from: a variable parameter received from the user terminal, a H/W key ID retrieved from a user information database by using a user ID received from the user terminal, and the first key, as recited in amended independent claims 1, 6 and 8.

Indeed, it is respectfully pointed out that Rosner et al discloses at column 5, lines 1-6 thereof (which the Examiner asserts discloses the generation of the second key of the present invention) that the partial keys are generated based on the public keys of the destination devices (which the Examiner apparently considers to correspond to the variable parameter of the present invention) and the private key associated with the source device (which the Examiner apparently considers corresponds to the H/W key ID of the present invention).<sup>1</sup> And it is respectfully submitted that the private key of the source

---

<sup>1</sup> It is not clear what key of Rosner et al the Examiner considers to correspond to the H/W key ID of the present invention. On pages 2 and 3 of the Office Action the Examiner refers to column 5, lines 1-6 and column 4, lines 30-35 of Rosner et al with respect to the H/W key ID. However, column 5, lines 1-6 of Rosner et al relate to the private key of the source device, whereas column 4, lines 30-35 of Rosner et al relates to the private keys of the destination devices.

Application No. 09/943,889  
Response to Office Action

Customer No. 01933

device is clearly not retrieved from a user information database by using a user ID received from the user terminal, in the manner of the H/W key ID of the present invention as recited in amended independent claims 1, 6 and 8.

In view of the foregoing, it is respectfully submitted that the present invention as recited in amended independent claims 1, 6 and 8, as well as claims 2, 4, 5, 7 and 9-12 respectively depending therefrom, clearly patentably distinguishes over Rosner et al, under 35 USC 103.

\* \* \* \* \*

Entry of this Amendment, allowance of the claims and the passing of this application to issue are respectfully solicited.

If the Examiner has any comments, questions, objections or recommendations, the Examiner is invited to telephone the undersigned for prompt action.

Respectfully submitted,

/Douglas Holtz/

Douglas Holtz  
Reg. No. 33,902

Frishauf, Holtz, Goodman & Chick, P.C.  
220 Fifth Avenue - 16<sup>th</sup> Floor  
New York, New York 10001-7708  
Tel. No. (212) 319-4900  
Fax No. (212) 319-5101  
DH:iv  
encs.